February 2013

Collective Defense: Applying Public Health Models to Internet Security

Key Points

- Malware and botnets enable cyber crime, costing consumers and business billions of dollars each year. In response, a collective defense across the Internet is needed to ensure a systematic approach to dealing with these threats. Improving the health of consumer devices connected to the Internet will benefit not only consumers, but the information technology ecosystem as a whole.

- One way to address issues of online security is to apply a model similar to the one society uses to address human illness. The public health model of identifying and controlling infectious diseases encompasses a number of concepts that can be applied to Internet security.

- Any effort to promote Internet health and security must be balanced with considerations of the social, legal, and economic issues of privacy, and designed not to impact economic activity adversely. An Internet health model will work as a collective defense only if it is accepted by society and if people are confident that their privacy will be protected.

BACKGROUND

Advances in online technology have led to remarkable global development, social change, and an evolution in the way businesses, civil society, and governments work from day to day. Unfortunately, these advances have been accompanied by a rise in online crime, which threatens to undermine the public trust. Today's leaders and decision makers must respond to this new reality with new ideas and solutions, and engage as partners in the public debate on Internet safety, privacy, and accountability.

The challenges are substantial and complex.

- Cyber threats have become more widespread, sophisticated, and difficult to characterize, having little in common in terms of origin, path, or impact. This calls for a myriad of responses and solutions worldwide.

- Botnets, the most insidious of malware, threaten infrastructure, and in turn endanger financial markets, military institutions, and national security.

- Individuals and organizations have a wide variety of choices to help defend their devices against cyber threats, including antimalware solutions, firewalls, and security updates. However, despite the broad availability of these technologies, they are not always fully deployed. Enterprises spend a great deal of time and money to manage risk with well-trained staff and sophisticated systems. Consumers, on the other hand, often lack the expertise and know-how to protect their devices themselves.

One way to address cyber threats is to model cyber security on efforts to address human illnesses. In a public health model, citizens must be aware of basic health risks and be educated on how to avoid them. In schools, for example, students may be required to be vaccinated before admission, warned if other students show symptoms, asked to stay at home if infected, and required to meet specified criteria for re-admission.

To improve the security of the Internet, governments and industry could similarly engage in systematic activities to improve and maintain the health of devices connected to the Internet. They could deploy people and technology to promote preventive measures, detect infected devices, and notify affected users. They could then help users repair malware-infected devices and take additional action to ensure that infected computers do not put other computers at risk.

Industry and governments have already begun such efforts. For example, the Internet Industry Association of Australia launched its voluntary Internet Service Provider (ISP) Code of Conduct. ISPs that use this system notify consumers with infected computers and offer them disinfection and repair tools. In Germany, the Anti-Botnet-Advisory Centre works in a similar way with local ISPs who notify and assist consumers whose computers are infected with malware. In Finland, TeliaSonera, an ISP serving 164 million customers, deploys an automated monitoring system to identify infected devices, alert their owners, and quarantine the devices from the network until they are cleaned.

MICROSOFT APPROACH

- Microsoft supports a collective cyber security defense similar to a public health model that limits the spread of human illness. Microsoft believes a similar model can be used by governments and IT industry leaders to more methodically prevent, detect, and treat computers infected with malware or botnets.
- This model is just a starting point. This vision can become a reality only with the support of consumers, government leaders, and privacy advocates, as well as ISPs and others in the industry.
- Microsoft works with the IT community to share information on malware and botnets, and to help assist affected customers.

POLICY CONSIDERATIONS

- Citizens the world over face more dangers online, while businesses and governments confront substantial cyber security issues. These call for collaborative solutions. Effective and far-reaching goals can be achieved only if all parties agree to an open exchange of ideas and a sustained commitment to work together to align social, economic, and political innovations and mount a collective defense against cyber threats.
- As with any international effort, every region will have differing sensitivities, so solutions must be socially acceptable and meet with public approval—especially when balancing security and privacy. Global progress on creating a safer online world merits coordination among industry, government, academics, and all societies worldwide and an open exchange of ideas about how better to protect the health of devices on the Internet.

Helpful Resources

Microsoft Global Security Strategy and Diplomacy Internet Health Site
aka.ms/gssd-health

Microsoft End to End Trust—Internet Health
aka.ms/internet-health

The Internet Health Model for Cybersecurity. EastWest Institute, 2012
www.ewi.info/internet-health